INTELLIGENCE UPDATE

Key players: cloud control and the colo advantage

Dr. Owen Rogers

9 Oct 2025

A recent Uptime Intelligence report shows how the US Cloud Act allows US law enforcement to access data held in most hyperscaler cloud environments, even when that data resides in other countries (see *In cloud and colo, whose laws rule the data*). With tensions still high between the US and Europe over NATO commitments and trade tariffs, some European organizations are concerned about potential extrajudicial access to their data (see *Europe will not abandon the hyperscalers*).

In contrast, colocation providers are not subject to the Cloud Act in the same way, as they do not manage or control data. Instead, they provide customers with space and power to support their own infrastructure, leaving the customer to manage the data.

Encryption can provide a solution for organizations that wish to use hyperscaler infrastructure without exposing data to potential access by US authorities. Without access to decryption keys, the cloud provider cannot provide law enforcement with a customer's original, unencrypted data, even if compelled to do so under the Cloud Act. However, vulnerability to the Cloud Act depends on the chosen key management model, which determines who has access to encryption keys.

The Cloud Act

This report provides an overview of Uptime Intelligence's understanding of the US Cloud Act regarding colocation facilities and cloud providers. However, it is not intended as legal advice, and organizations should seek specialist guidance before pursuing any course of action.

The Cloud Act, or more formally, the US Stored Communications Act (18 USC 2713), is recapped here, as its specific wording raises implications for both cloud and colocation providers. A fuller explanation can be found in a previous update (see *In cloud and colo, whose laws rule the data*):

"A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or

electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States."

All hyperscalers encrypt data at rest

All major cloud providers — AWS, Google, Microsoft, Oracle and IBM — encrypt “data at rest” as standard on most services. The same is true for many European cloud providers, such as OVHcloud, Scaleway, Exoscale, IONOS and UpCloud. For example, data stored in object storage is encrypted by the cloud provider as soon as it is uploaded. When that data is accessed through a legitimate, authenticated channel (such as a secure API call), the cloud provider decrypts it and delivers it to the user or application. To perform decryption, a key is required. In this scenario, the cloud provider owns and manages the key, making the process invisible to both the customer and the end user.

Such standard encryption would fall under the Cloud Act. First, if the data is in the “possession” or “custody” of the cloud provider, the Act explicitly allows law enforcement to access it. Second, because the provider can manipulate the data — by encrypting and decrypting it — the data is considered to be under the provider’s “control.” Thus, the cloud provider can not only be required to pass the key to law enforcement authorities, but also be compelled to use that key, as the controller, to decrypt the data on their behalf.

Key management is still vulnerable

Some customers prefer to manage their own encryption keys. This can be achieved using a key management service (KMS), which enables users to create, store and control access to encryption keys. A KMS can automate encryption and decryption processes across cloud services while keeping keys managed within the provider's infrastructure. Customers can typically choose how much control of the backend management is passed to the cloud provider. Hyperscaler offerings include AWS KMS, Azure Key Vault, Google Cloud KMS, IBM Key Protect and Oracle Vault. The cloud provider then uses the keys stored in the KMS to automatically encrypt and decrypt data.

The cloud provider stores the encryption keys in its own data center and infrastructure. As a result, the cloud provider retains both possession and control of the key data. Consequently, both the customer data and encryption key data are vulnerable to US enforcement access, regardless of where the data is stored.

Dedicated hardware protects

Ultimately, the only way to prevent US authorities from accessing data held in US-based hyperscalers is to retain custody and control of the encryption keys.

A hardware security module (HSM) is a dedicated physical device that securely generates, stores and manages cryptographic keys, enabling encryption and decryption operations without exposing the keys to external systems or users. A cloud provider would use an HSM to manage its keys in standard KMS encryption, but — crucially — this occurs on a shared basis, hidden from customer access and visibility.

This centralized HSM is managed by the cloud provider for all their customers' keys. As a shared platform, the cloud provider retains control of the key data, which means it is potentially vulnerable to US access.

If the cloud customer is provisioned with a dedicated HSM to manage their keys, their data may be protected from external access. In this case, the cloud provider is almost acting as a colocation host — providing the space and power for the appliance, as well as the appliance itself, but without having the ability to access the stored data. Even though the cloud provider has control of the hardware, it does not have control of the data contained within — even if it wanted to, the provider would not be able to access the data. The customer, however, remains responsible for ensuring that the device is configured correctly and secured at an operating system level to prevent remote access from unauthorized parties.

While it is possible the cloud provider may attempt to hack into the appliance, it is not an easy process. Most HSMs are certified by FIPS (a US government standard) to ensure that if someone attempts to tamper with the device — physically or digitally — it will automatically shut down or erase sensitive data to prevent unauthorized access. Additionally, the cloud provider would not be required to do this because, according to the wording of the Cloud Act, they are not in control of the data — only the appliance. To gain access to a device located in a European country, US authorities would need to pursue a physical seizure through a local court order. Without local law enforcement cooperation, carrying out a seizure would be a complex process.

External key management

The most robust option is to host an HSM in a private data center or colocation facility while utilizing an external key management service (XKS). In this setup, all encryption keys and key management are entirely outside the cloud provider's control. The cloud provider communicates with the HSM (on-premises) to authorize operations, but no key information is exchanged with the cloud provider. This approach is a hybrid application that requires both public cloud and on-premises infrastructure to operate. In this scenario, the Cloud Act legislation would generally not provide a route for government access to the key data.

Colocation providers are typically not subject to the Cloud Act because they are not "remote computing services" under US law and do not manage customer data or infrastructure. Colocation facilities owned by US organizations but operating under European legal entities are unlikely to fall within the scope of Cloud Act obligations unless they directly manage customer data, such as through a managed service.

Is it worth it?

As discussed in a previous report, most European enterprises will not make material changes to their cloud estates as a result of ongoing tensions with the US (see *Europe will not abandon the hyperscalers*). Most organizations will likely decide that the likelihood and potential impact of extrajudicial data access are small enough that relocating their workloads is not worth the cost or complexity.

Enterprises are drawn to the public cloud because of the convenience and scalability of outsourcing data center, infrastructure and platform management to a third party. For many, giving up this level of flexibility is simply too great a trade-off for such a relatively small risk.

However, for other organizations — such as governmental bodies, where the repercussions of extrajudicial data access are much broader — additional mitigation measures may be necessary. Yet, for encryption to serve as a viable safeguard against the Cloud Act, the customer will have to sacrifice some convenience. This is especially true of XKS, where customers need to use private or colocation facilities alongside the public cloud — a configuration that is usually more complex to implement and manage than when hosted in a single location.

In some cases, it may be simpler and more secure to move all the applications to on-premises infrastructure or to a Europe-headquartered cloud provider. This approach avoids any Cloud Act jurisdiction and removes the need to establish secure and resilient communication between the public cloud and dedicated key management infrastructure.

However, for large estates, a hybrid model makes sense. Multiple resilient KMSs, distributed across various locations, can protect data stored in the public cloud across multiple geographic regions. This model enables organizations to utilize hyperscaler cloud infrastructure near users and take advantage of cloud services and capabilities on demand, while protecting data from potential US government access.

External key management presents an opportunity for colocation providers to host key management infrastructure or even operate the hardware as a managed service. Colocation providers that collaborate with cloud provider networks are ideally placed to host external key management infrastructure. With their proximity to cloud providers, such colocation facilities help reduce latency between public cloud applications and external key management, improving performance. At the same time, they also protect key infrastructure from the Cloud Act, thereby enabling organizations to leverage public cloud scalability without compromising security.

Several colocation providers already host external key management infrastructure to support customers seeking data sovereignty and protection from the Cloud Act. Equinix (via its SmartKey service in partnership with Fortanix), Digital Realty (with ServiceFabric) and Interxion enable secure, low-latency connections to hyperscalers, making them suitable for hybrid encryption setups.

The Uptime Intelligence View

Cloud provider encryption offers only limited protection against the Cloud Act. Any data managed by a US-based cloud provider, regardless of its location, is susceptible to the Act, including encryption key data. Locating data in a colocation facility or a European cloud provider can help mitigate this risk. However, for organizations that require hyperscaler cloud, the most robust option is to manage their own keys using dedicated hardware, either located in the cloud provider’s environment, a private data center or a colocation facility. With ongoing geopolitical tensions between the US and Europe, colocation providers have an opportunity to host more applications and key management systems outside US jurisdiction.

ABOUT THE AUTHOR

Dr. Owen Rogers

Dr. Owen Rogers is Uptime Institute’s Senior Research Director of Cloud Computing. Dr. Rogers has been analyzing the economics of cloud for over a decade as a chartered engineer, product manager and industry analyst. Rogers covers all areas of cloud, including AI, FinOps, sustainability, hybrid infrastructure and quantum computing.

orogers@uptimeinstitute.com

About Uptime Institute

Uptime Institute is the Global Digital Infrastructure Authority. Its Tier Standard is the IT industry's most trusted and adopted global standard for the proper design, construction, and operation of data centers – the backbone of the digital economy. For over 25 years, the company has served as the standard for data center reliability, sustainability, and efficiency, providing customers assurance that their digital infrastructure can perform at a level that is consistent with their business needs across a wide array of operating conditions.

With its data center Tier Standard & Certifications, Management & Operations reviews, broad range of related risk and performance assessments, and accredited educational curriculum completed by over 10,000 data center professionals, Uptime Institute has helped thousands of companies, in over 100 countries to optimize critical IT assets while managing costs, resources, and efficiency.